CLAIMS:

1. A method of controlling access to data stored on a device, the method comprising the steps of:

generating a symmetric key;

encrypting said data by performing a first mathematical operation on said data, said first mathematical operation associated with said symmetric key;

intercepting control signals requesting access to said data;

decrypting said data by selectively performing a complimentary second mathematical function on said data, said complimentary second mathematical operation associated with said symmetric key; and

maintaining data in encrypted form until access thereto is requested.

2. The method of claim 1, wherein said data includes logically linked data records to form a database.

3. The method of claim 1, wherein said symmetric key is generated from random data received from recording stylus movements performed by a user.

4. The method of claim 3, wherein said stylus movements form a bit image, said bit image being used in the generation of said symmetric key.

5. A method of securing data on a personalized device comprising the steps of:

generating a secure symmetric key;

encrypting said data with said secure symmetric key, in accordance with an the predetermined algorithm;

storing said data in encrypted form until a request for read and write access is made;

decrypting said data with said secure symmetric key for read and write access; and

encrypting said secure symmetric key with a public key.

6. A method of claim 5, whereby the step of generating a secure symmetric key includes a plurality of different degrees of key length, said key length associated with level of security.

7. The method of claim 6, wherein said predetermined algorithm is selected from a

group of mathematical operations.

8. The method of claim 7, wherein said mathematical operations are DES, triple-DES, Skipjack and Rijndael.

9. The method of claim 7 and 8, wherein said level of security is depends on selected mathematical operation.

10. A method of securing stored data on a mobile computing device and controlling access to said stored data by a user, said method comprising the steps of:

associating said stored data with a plurality of unique identifiers;

encrypting said stored data by performing a mathematical operation thereon, and maintaining said stored data in encrypted format;

initiating a first call to access said stored data to a processor, said first call including a unique identifier;

intercepting said first call to assess level of privilege associated with said user,

manipulating said first call in accordance with said level of privilege to generate a second call to said processor, said second call including said unique identifier;

communicating second call to said stored data to access said stored data associated with said unique identifier;

decrypting said stored data associated with said unique identifier by performing a complimentary mathematical operation to said stored data, said step of decrypting said stored data in accordance with said level of privilege;

communicating said decrypted stored data associated with said unique identifier to said user; and

encrypting said stored data with said mathematical operation subsequent to access by said user.

11. The method of claim 10, wherein the step of controlling access includes steps of:

a client application retrieving a handle to a record in a memory segment via a first call;

passing the handle to second call to lock said memory segment associated with the handle;

the handle returning a pointer to client application, said pointer associated with said locked memory segment;

the client application reading or writing to the locked memory segment;

passing said handle to third call to unlock the locked memory segment, upon completion of said reading or writing.

12. The method of claim 11, wherein the step of controlling access further includes a step of optimizing access to the data records, said step including maintaining an access list of recently accessed pointers and handles.

13. A improved data security system on a portable device, said system having:

a data storage unit for storing said data, said data having data records and said each of said data records associated with a unique identifier;

a processor for executing predetermined instructions belonging to a predetermined instruction set, said instruction set associated with access instructions to said records;

a patch for preventing execution of received predetermined instructions, and for verifying origin of said received instructions, and for further generating new instructions associated with said received predetermined instructions, upon verification thereof;

whereby a data record is accessed by initiating an instruction with the unique identifier of the data record to be accessed to the processor, said instruction being intercepted and converted into a new instruction by said patch upon verification of origin.

14. A method of claim 1, wherein the method further includes the steps of synchronizing a database on said device with a database on another device.